Xerox System Integration Standard

SECONDARY CREDENTIALS FORMATS

XNSS 258605
May 1986

XEROX

Notice

This *Xerox System Integration Standard* describes Secondary Credentials Formats.

This document is being provided for informational purposes only. Xerox makes no warranties or representations of any kind relative to this document or its use, including the implied warranties of merchantability and fitness for a particular purpose. Xerox does not assume any responsibility or liability for any errors or inaccuracies that may be contained in the document, or warrant that the use of the information herein will produce results in an intended manner.

The information contained herein is subject to change without any obligation of notice on the part of Xerox.

All text and graphics prepared on the Xerox 8010 Information System.

Printed in U.S.A. Publication number: 610P50678

PREFACE

This document is one of the family of publications that describe the network protocols underlying Xerox Network Systems (XNS).

Xerox Network Systems comprise a variety of digital processors interconnected by means of a variety of transmission media. System elements communicate both to transmit information between users and to share resources economically. For system elements to communicate with one another, certain standard protocols must be observed.

Comments and suggestions on this document and its use are encouraged. Please address communications to:

Xerox Corporation
Xerox Systems Institute (XSI) Office
475 Oakmead Parkway, Bldg. 5
Sunnyvale, California 94086

TABLE OF CONTENTS

1. INTRODUCTION

This document defines the types and formats of certain secondary credentials. Secondary credentials are arbitrary authentication data required by certain recipients, such as those implemented on foreign operating systems. The formats are defined in terms of Courier [1] data types.

1.1 Purpose

The format of the secondary credentials required varies from one recipient to another, as the requirements for auxiliary authentication data vary. In order to communicate successfully with a recipient, the initiator must supply any secondary credentials in the proper format. Secondary credentials formats are defined here as an aid to communicating the desired format from the recipient to the initiator. In addition to specifying the structure of the values, this document describes how the values are intended to be used. This information is required for sharing of these formats. Format numbers for secondary credentials are administered as described in Appendix B.

1.2 Documentation conventions

Courier text and examples are depicted in special fonts, and generally conform to a certain style. The rules and style are set forth below.

Throughout this document, special fonts are used to depict Courier text instead of using quote marks or other delimiters. This convention also aids the eye in discriminating between Courier text and the exposition. Items in THIS FONT indicate elements of the Courier language and are almost always in upper case. **This font** indicates items that are defined using the Courier language.

Identifiers that are defined in this protocol (as opposed to being defined by Courier) will have their first letter capitalized if they are the name of a type, error, or procedure; identifiers with a lower case first letter are usually the names of variables, arguments, or results.

1.3 Document organization

Chapter 2 of this document defines the formats of the standard secondary credentials types. Appendix A lists other documents which supplement the specification. Appendix B explains how to acquire a block of secondary credentials types.

Secondary credentials consist of a sequence of secondary items, each of which contains a component of the secondary credentials information. This document defines secondary items and how to group them into the secondary credentials required by hybrid hosts. Users of secondary credentials may use the administrative procedures defined in Appendix B to register new secondary items.

```
Secondary: TYPE = SEQUENCE 10 OF SecondaryItem;
```

Up to 10 secondary items may be grouped as the constituents of a value of secondary credentials.

2.1 Secondary items

Each secondary item consists of a type and a value.

```
SecondaryItemType: TYPE = LONG CARDINAL;

SecondaryItem: TYPE = RECORD [
    type: SecondaryItemType,
    value: SEQUENCE OF UNSPECIFIED];
```

Also associated with each secondary item type is a recommendation as to the privacy of the item. This privacy level can be used by clients to determine, for example, whether a user-supplied value for an item should be echoed to the user. This privacy level is specified in this document, but is not reflected in any data structures—that is, the privacy level associated with a secondary item type is documented, but not transmitted.

```
systemPassword: SecondaryItemType = 1;
SystemPassword: TYPE = STRING;                    -- value is private
```

The **SystemPassword** is used to control access to the hybrid system itself. When used, it generally is applied before other secondary items. If a system password exists, it normally has one value for the entire set of users.

```
userName: SecondaryItemType = 2;
UserName: TYPE = STRING;                          -- value is not private

userPassword: SecondaryItemType = 3;
UserPassword: TYPE = STRING;                      -- value is private

userPassword2: SecondaryItemType = 4;
UserPassword2: TYPE = STRING;                     -- value is private
```

The **UserName** and **UserPassword** identify the user to the hybrid operating system. In those cases in which a secondary password is required by the operating system, **UserPassword2** is used. Although not a requirement, a user normally has a single set of values for **UserName** and **UserPassword(2)** on a given system element.

```
userServiceName: SecondaryItemType = 5;
UserServiceName: TYPE = STRING;                    -- value is not private

userServicePassword: SecondaryItemType = 6;
UserServicePassword: TYPE = STRING;                -- value is private

userServicePassword2: SecondaryItemType = 7;
UserServicePassword2: TYPE = STRING;               -- value is private
```

In certain cases, access to a service running on the operating system is controlled, in addition to controlling access to the operating system itself. In these cases, **UserServiceName** , **UserServicePassword**, and **UserServicePassword2** identify the user to the individual service.

```
accountName: SecondaryItemType = 8;
AccountName: TYPE = STRING;                        -- value is not private

accountPassword: SecondaryItemType = 9;
AccountPassword: TYPE = STRING;                    -- value is private

accountPassword2: SecondaryItemType = 10;
AccountPassword2: TYPE = STRING;                   -- value is private
```

In some cases, the entity which is considered to be logged on is not a user, but an account. In these cases, values for **AccountName**, **AccountPassword**, and **AccountPassword2** can be supplied.

Alternatively, accounting information may be required at the time a user is authenticated. In this case, **AccountName** may be used to transmit this information.

```
secondaryString: SecondaryItemType = 1000;
SecondaryString: TYPE = STRING;                    -- value is not private

privateSecondaryString: SecondaryItemType = 1001;
PrivateSecondaryString: TYPE = STRING;             -- value is private
```

SecondaryString and **PrivateSecondaryString** may be used to transmit secondary credentials information which is not of one of the aforementioned types. This is useful if a service has requirements for credentials which are not standardized.

A. REFERENCES

The following documents supplement this protocol specification.

[1] Xerox Corporation. *Courier: The Remote Procedure Call Protocol.* Xerox System Integration Standard. Stamford, Connecticut. December 1981. XSIS 038112.
This reference defines the Courier language, in terms of which the secondary credentials formats are defined.

B. TYPE ASSIGNMENT PROCEDURES

As stated in this document, format types are assigned 32-bit numbers that are unique throughout the distributed system. The number space is administered by Xerox Corporation. To obtain a block of numbers, submit a written request to:

Xerox Corporation
Xerox Systems Institute (XSI) Office
475 Oakmead Parkway, Bldg. 5
Sunnyvale, California 94086

Implementors are encouraged to apply for unique blocks of numbers for their particular applications. Uniqueness allows systems to freely interconnect without having to worry about overlapping values.

Format numbers should be used with economy, as the total number of blocks is limited. If an implementation is using a large quantity of these format type numbers, the designer has probably misunderstood their purpose.